



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/006,465	12/06/2001	Bahman Qawami	M-9913-1 US	3583

36257 7590 04/29/2005

PARSONS HSUE & DE RUNTZ LLP
655 MONTGOMERY STREET
SUITE 1800
SAN FRANCISCO, CA 94111

EXAMINER

GELAGAY, SHEWAYE

ART UNIT PAPER NUMBER

2133

DATE MAILED: 04/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/006,465

Applicant(s)

QAWAMI ET AL.

Examiner

Shewaye Gelagay

Art Unit

2133

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 06 December 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-39 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-39 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 06 December 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☒ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>12/16/01, 10/25/04, 1/31/05, 2/10/05</u> | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-39 have been examined.

Oath/Declaration

2. The oath or declaration is defective. A new oath or declaration in compliance with 37 CFR 1.67(a) identifying this application by application number and filing date is required. See MPEP §§ 602.01 and 602.02.

The oath or declaration is defective because: It is not signed by the inventors.

Specification

3. The disclosure is objected to because of the following informalities: Related application's serial number is missing on pages 1 and 2.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. The term "about" in claims 5, 12, 22 and 24 is a relative term which renders the claims indefinite. The term "about" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. The term

Art Unit: 2133

"about" has to be explicitly defined in claims 5, 12, 22 and 24 so that there would not be any ambiguity.

Claim Rejections - 35 USC § 101

1. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and, *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

2. Claims 1-7 and 13-39 are provisionally rejected under the judicially created doctrine of double patenting over claims 7, 22, 23 and 31 of copending Application No. 10/006,554. Although the conflicting claims are not identical, they are not patentably distinct from each other because the application '554 teaches all the claims limitation except the differences that are underlined in the following table:

10/006465	10/006554
1. A method of accessing an encrypted track on a removable media with a device, the track comprising frames having content, the method comprising: authorizing the media; decrypting the track by a process comprising: (a) calculating a media unique key; and thereafter (b)	7. The software program of claim 1 wherein decrypting the audio or video content comprises: (a) calculating a media unique key; and thereafter (b) decrypting a title key stored in the memory of the device with the media unique key; and thereafter (c) decrypting a group of frames; and

<p>decrypting a title key stored in the memory of the device with the media unique key; and thereafter (c) decrypting a group of frames; and thereafter (d) deleting the decrypted title key; (e) deleting the media unique key; and (f) repeating (a) through (e) until the entire track is completed.</p>	<p>thereafter (d) deleting the decrypted title key; (e) deleting the media unique key; and (f) repeating (a) through (e) until the entire track is completed.</p> <p>22. The system of claim 21, wherein the one or more keys are in a decrypted state for the time it takes to decrypt and process less than one second to about five seconds of decoded content.</p>
<p>13. A system for enabling a device to read an encrypted file having encrypted content from a media, and to write an encrypted file having encrypted content to a media, the system comprising: <u>a computing unit</u>, and a system memory; interface means for receiving commands from the device; secure dynamic decryption means configured to: (a) copy an encrypted title key from the media to a memory of the device, (b) decrypt the encrypted title key, (c) decrypt a portion of encrypted content with the decrypted title key, (d) delete the decrypted title key, and (e) repeat a-d such until all of the content of the file has been decrypted, and <u>wherein the decrypted title keys reside in and are accessible only to the secure means of the system.</u></p>	<p>23. A system enabling a portable device to access encrypted music on a memory storage device comprising: one or more application programming interfaces configured to: receive a plurality of commands from a user interface of the portable device; and send commands to an isolated security engine, the isolated security engine configured to: receive commands from the application programming interface; copy encrypted keys and encrypted content from the memory storage device to a memory of the portable device; decrypt the keys; decrypt the content using the decrypted keys; and thereafter delete the decrypted keys.</p>
<p>20. A system that enables a device to decrypt a file having encrypted content on a secure medium, the system comprising: one or more user interface modules for receiving commands from the device; an applications programming interface for receiving the commands from the one or more user interface modules and managing the retrieval and storage of encrypted content from the secure medium; a security engine for decrypting the encrypted content and the one or more encrypted keys sent from the secure</p>	<p>31. A software system that enables a device to access content on a secure medium comprising: one or more user interface modules for receiving commands from the device; an applications programming interface for receiving the commands from the user interface module(s) and managing the retrieval and storage of both encrypted and non encrypted content from the secure medium; a security engine for decrypting the encrypted content and encrypted keys sent from the secure medium to memory</p>

medium to a memory of the device, the decrypted keys used to decrypt the encrypted content, wherein the one or more keys are contained in an encrypted data segment, and the security engine (a) decrypts one or more of the keys, (b) <u>decrypts a portion of the encrypted content using the one or more decrypted keys, and</u> (c) deletes the one or more decrypted keys, and (d) repeats (a)-(c) until all portions of the content are decrypted.	of the device, the decrypted keys used to decrypt the encrypted content, and wherein one or more of the keys are contained in a first encrypted data segment, and encrypted content is contained in a second encrypted data segment, and <u>the security engine buffers and decrypts a portion of the first data segment, buffers and decrypts the second data segment, and thereafter deletes the</u> decrypted one or more keys before decrypting the, such that decrypted keys are in a decrypted state for the time it takes to decrypt less than one to about five seconds of content.
--	---

a. Both '465 (claim 1) and '554 (claims 7 and 22) teach accessing an encrypted content on a media by authorizing the media and decrypting the content.

b. Both '465 (claim 13) and '554 (claim 23) teach a system of enabling a device to read and access encrypted content on a media or memory storage. The only exception is claim 13 in '465 has a computing unit. However, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the device disclosed by '554 to include a computing unit. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so because the device disclosed by '554 has to have a computing unit in order to perform decryption, copying and deletion.

c. Both '465 (claim 20) and '554 (claim 31) teach a system of enabling a device to read and access encrypted content on a media or memory storage. The only exception is claim 20 in '465 the decryption process is performed by decrypting only a portion of the encrypted content using one or more decrypting keys while claim 31 in

Art Unit: 2133

'554 has a buffer and decrypts a portion of the first data segment, buffers and decrypts the second data segment. However, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by '554 to include the decryption process is performed by decrypting only a portion of the encrypted content using one or more decrypting keys. This modification would have been obvious because, a person having ordinary skill in the art would have been motivated to do so because decrypting only a portion of the encrypted content using one or more decrypting keys would like using a buffer would facilitate the decryption process thereby allowing fast access to the encrypted content.

This is a provisional double patenting rejection since the conflicting claims have not in fact been patented.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to

Art Unit: 2133

consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

7. Claims 1, 5-7 and 13-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tagawa et al. (hereinafter Tagawa) United States Letter Patent Number 6,832,293 in view of Dolan et al. (hereinafter Dolan) United States Letter Patent Number 5,604,801.

As per claim 1:

Tagawa teaches a method of accessing an encrypted track on a removable media with a device, the track comprising frames having content, the method comprising: authorizing the media; decrypting the track by a process comprising:

(a) calculating a media unique key; (Col. 9, lines 20-21) and thereafter

(b) decrypting a title key stored in the memory of the device with the media unique key; (Col. 9, lines 14-29) and thereafter

(c) decrypting a group of frames; (Col. 5, lines 65-66; Col. 83, lines 51-52 and lines 66-67; Col. 90, lines 10-18; Col. 94, lines 22-32)

Tagawa does not explicitly disclose (d) deleting the decrypted title key; and (e) deleting the media unique key; and (f) repeating (a) through (e) until the entire track is completed.

Dolan in analogous art, however, discloses (d) deleting the decrypted title key; (Col. 3, lines 11-14) and (e) deleting the media unique key; (Col. 3, lines 11-14) and (f) repeating (a) through (e) until the entire track is completed. (Col. 3, lines 11-14; ...after use; *after use is interpreted as until the entire track is completed*)

Art Unit: 2133

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Tagawa to include deleting the decrypted title key; deleting the media unique key; and repeating (a) through (e) until the entire track is completed. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Dolan (Col. 2, lines 27-28) in order not to compromise the decryption key.

As per claim 5:

Tagawa and Dolan teach all the subject matter as discussed above. In addition, Tagawa further discloses a method wherein the group of frames comprises less than one to about five seconds of content in a decoded or decompressed form. (Col. 15, lines 59-65)

As per claim 6:

Tagawa and Dolan teach all the subject matter as discussed above. In addition, Tagawa further discloses a method wherein decrypting the track comprises decrypting one or more files, the files comprising the frames. (Col. 5, lines 65-66; Col. 13, lines 8-11; Col. 83, lines 51-52 and lines 66-67; Col. 90, lines 10-18; Col. 94, lines 22-32)

As per claim 7:

Tagawa and Dolan teach all the subject matter as discussed above. In addition, Tagawa further discloses a method comprising decoding and decompressing the track. (Col. 42, lines 52-56; Col. 55, lines 1-5)

As per claim 13:

Art Unit: 2133

Tagawa teaches a system for enabling a device to read an encrypted file having encrypted content from a media, and to write an encrypted file having encrypted content to a media, the system comprising:

a computing unit, and a system memory; (Figure 52, items 3, 4 and 10)

interface means for receiving commands from the device; (Col. 11, line 67; Col. 12, line 1; Col. 41, lines 20-21)

secure dynamic decryption means configured to:

(a) copy an encrypted title key from the media to a memory of the device, (Col. 12, lines 16-61; Col. 46, lines 10-11)

(b) decrypt the encrypted title key, (Col. 9, line 16-24)

(c) decrypt a portion of encrypted content with the decrypted title key, (Col. 12, lines 1-12; Col. 41 lines 25-29)

Tagawa does not explicitly disclose (d) delete the decrypted title key, and (e) repeat a-d such until all of the content of the file has been decrypted, and wherein the decrypted title keys reside in and are accessible only to the secure means of the system.

Dolan in analogous art, however, discloses (d) delete the decrypted title key, (Col. 3, lines 11-14) and (e) repeat a-d such until all of the content of the file has been decrypted, and wherein the decrypted title keys reside in and are accessible only to the secure means of the system. (Col. 3, lines 11-14)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Tagawa to

Art Unit: 2133

include (d) delete the decrypted title key, and (e) repeat a-d such until all of the content of the file has been decrypted, and wherein the decrypted title keys reside in and are accessible only to the secure means of the system. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Dolan (Col. 2, lines 27-28) in order not to compromise the decryption key.

As per claim 14:

Tagawa and Dolan teach all the subject matter as discussed above. In addition, Tagawa further discloses a system wherein the title key is in a decrypted state for the time it takes to decrypt 5 seconds or less of content in a decompressed and decoded state when played back. (Col. 15, lines 59-65)

As per claims 15 and 26:

Tagawa and Dolan teach all the subject matter as discussed above. In addition, Tagawa further discloses a system comprising a digital signal processor. (Col. 8, lines 41-50; Col. 55, lines 1-5)

As per claims 16 and 27:

Tagawa and Dolan teach all the subject matter as discussed above. In addition, Tagawa further discloses a system wherein the interface means and secure dynamic decryption means are stored in a system memory of the device. (Col. 41, lines 20-33)

As per claims 17 and 28:

Tagawa and Dolan teach all the subject matter as discussed above. In addition, Tagawa further discloses a system wherein the interface means and secure dynamic

Art Unit: 2133

decryption means are executed by the computing unit. (Col. 41, lines 32-33)

As per claims 18:

Tagawa and Dolan teach all the subject matter as discussed above. In addition, Tagawa further discloses a system wherein the secure dynamic decryption means is stored in memory of the digital signal processor, and executed by the digital signal processor. (Col. 41, lines 32-33)

As per claim 19:

Tagawa and Dolan teach all the subject matter as discussed above. In addition, Tagawa further discloses a system wherein the interface means is executed by the digital signal processor. (Col. 41, lines 32-33)

As per claim 20:

Tagawa teaches a system that enables a device to decrypt a file having encrypted content on a secure medium, the system comprising:

one or more user interface modules for receiving commands from the device;
(Col. 11, line 67; Col. 12, line 1; Col. 41, lines 20-21)

an applications programming interface for receiving the commands from the one or more user interface modules and managing the retrieval and storage of encrypted content from the secure medium; (Col. 11, line 67; Col. 12, line 1; Col. 41, lines 20-21)

a security engine for decrypting the encrypted content and the one or more encrypted keys sent from the secure medium to a memory of the device, the decrypted keys used to decrypt the encrypted content, (Col. 9, lines 16-24; Col. 12, lines 1-12; Col. 41 lines 25-29) wherein

Art Unit: 2133

the one or more keys are contained in an encrypted data segment, and the security engine (a) decrypts one or more of the keys, (Col. 9, line 16-24; Col. 12, lines 16-61) (b) decrypts a portion of the encrypted content using the one or more decrypted keys, (Col. 12, lines 1-61; Col. 41 lines 25-29) and

Tagawa does not explicitly disclose (c) deletes the one or more decrypted keys, and (d) repeats (a)-(c) until all portions of the content are decrypted.

Dolan in analogous art, however, discloses (c) deletes the one or more decrypted keys, (Col. 3, lines 11-14) and (d) repeats (a)-(c) until all portions of the content are decrypted. (Col. 3, lines 11-14)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Tagawa to include (c) deletes the one or more decrypted keys, and (d) repeats (a)-(c) until all portions of the content are decrypted. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Dolan (Col. 2, lines 27-28) in order not to compromise the decryption key.

As per claim 21:

Tagawa and Dolan teach all the subject matter as discussed above. In addition, Tagawa further discloses a system wherein the content is encoded in the AAC, MP3 or WMA format. (Col. 55, lines 1-5)

As per claim 22:

Art Unit: 2133

Tagawa and Dolan teach all the subject matter as discussed above. In addition, Tagawa further discloses a system wherein the one or more keys are in a decrypted state for the time it takes to decrypt and process less than one second to about five seconds of decoded content. (Col. 15, lines 59-65)

As per claim 23:

Tagawa and Dolan teach all the subject matter as discussed above. In addition, Tagawa further discloses a system wherein the data segment comprising the one or more encrypted keys is buffered and decrypted in fractional portions. (Col. 9, lines 16-24; Col. 12, lines 1-12; Col. 41 lines 25-29)

As per claim 24:

Tagawa and Dolan teach all the subject matter as discussed above. In addition, Tagawa further discloses a system wherein the fractional portion is about 512 bytes. (Col. 17, lines 60-64)

As per claim 25:

Tagawa and Dolan teach all the subject matter as discussed above. In addition, Tagawa further discloses a system wherein the device comprises a computing unit, system memory, and a hardware interface. (Col. 41, lines 32-33)

As per claim 29:

Tagawa and Dolan teach all the subject matter as discussed above. In addition, Tagawa further discloses a system wherein the system is stored in RAM of the digital signal processor. (Col. 41, lines 38-42)

As per claim 30:

Art Unit: 2133

Tagawa and Dolan teach all the subject matter as discussed above. In addition, Tagawa further discloses a system wherein a portion of the system is stored in the system memory of the device and a portion of the system is stored in RAM of the digital signal processor. (Col. 41, lines 38-42)

As per claim 31:

Tagawa and Dolan teach all the subject matter as discussed above. In addition, Tagawa further discloses a system wherein the portion of the system stored in the RAM of the digital signal processor is executed by the digital signal processor. (Col. 41, lines 32-33 and lines 38-42)

As per claim 32:

Tagawa and Dolan teach all the subject matter as discussed above. In addition, Tagawa further discloses a system wherein the portion of the system stored in the RAM of the digital signal processor comprises the security engine. (Col. 41, lines 32-33 and lines 38-42)

8. Claims 2-4, 8-12 and 38-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tagawa et al. (hereinafter Tagawa) United States Letter Patent Number 6,832,293 in view of Dolan et al. (hereinafter Dolan) United States Letter Patent Number 5,604,801 and further in view of Ansell et al. (hereinafter Ansell) United States Letter Patent Number 6,367,019.

As per claim 2:

Tagawa and Dolan teach all the subject matter as discussed above. In addition, Tagawa further discloses a method wherein authorizing the media comprises:

Art Unit: 2133

calculating a media key; (Col. 9, lines 20-21) and thereafter

calculating a media unique key from the media key; (Col. 9, lines 20-21)

In addition, Dolan further discloses deleting the media key; (Col. 3, lines 11-14) and thereafter deleting the media unique key. (Col. 3, lines 11-14)

Both references do not explicitly disclose a method of calculating a session key from the media unique key.

Ansell in analogous art, however, discloses calculating a session key from the media unique key. (Col. 7, line 19; *calculating is interpreted as decrypting, the interpretation is given based on the description given on the disclosure*)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Tagawa and Dolan to include calculating a session key from the media unique key. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Ansell (Col. 7, lines 20-22) in order not to have a secure communication between the media and the device.

As per claim 3:

Tagawa and Dolan teach all the subject matter as discussed above. In addition, Tagawa further discloses a method wherein authorizing the media comprising: copying the singly encrypted title key from the media into a memory of the device. (Col. 12, lines 16-61; Col. 46, lines 10-11)

Both references do not explicitly disclose decrypting a doubly encrypted title key stored in the media with a session key calculated while authorizing the media to produce a singly encrypted title key.

Ansell in analogous art, however, discloses decrypting a doubly encrypted title key stored in the media with a session key calculated while authorizing the media to produce a singly encrypted title key. (Col. 7, line 19)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Tagawa and Dolan to include decrypting a doubly encrypted title key stored in the media with a session key calculated while authorizing the media to produce a singly encrypted title key. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Ansell (Col. 7, lines 20-22) in order not to have a secure communication between the media and the device.

As per claim 4:

Tagawa, Dolan and Ansell teach all the subject matter as discussed above. In addition, Tagawa further discloses a method wherein calculating the media key comprises:

(a) reading a first record of a media key block from a buffer; (Col. 12, lines 16-61; Col. 46, lines 10-11)

(b) updating the buffer offset based on the length and type of the first record; (Col. 12, lines 16-61; Col. 46, lines 14-16)

Art Unit: 2133

(c) reading another record of the media key block at the updated buffer offset;
(Col. 12, lines 16-61; Col. 25, lines 7-11; Col. 46, lines 14-16) and

(d) repeating (a)-(c) until all necessary records of the media key block are read and the media key is calculated. (Col. 12, lines 1-12; Col. 41 lines 25-29)

As per claim 8:

Tagawa teaches a method of accessing an encrypted data file on a removable media with a device, the data file comprising frames having content, the method comprising: authorizing the media for a user session by a process comprising:

calculating a media key; (Col. 9, lines 20-21) and thereafter

calculating a media unique key from the media key; (Col. 9, lines 20-21) and thereafter

copying the singly encrypted title key from the media into a memory of the device; (Col. 12, lines 16-61; Col. 46, lines 10-11) and

decrypting the file by a process comprising:

(a) calculating the media unique key; (Col. 9, lines 20-21) and thereafter

(b) decrypting the title key stored in the memory of the device with the media unique key; (Col. 9, lines 20-21) and thereafter

(c) decrypting a group of frames; (Col. 5, lines 65-66; Col. 83, lines 51-52 and lines 66-67; Col. 90, lines 10-18; Col. 94, lines 22-32) and thereafter

Tagawa does not explicitly disclose a method of (d) deleting the decrypted title key; (e) deleting the media unique key; and (f) repeating (a) through (e) until the entire file is completed.

Dolan in analogous art, however, discloses (d) deleting the decrypted title key; (Col. 3, lines 11-14) and (e) deleting the media unique key; (Col. 3, lines 11-14) and (f) repeating (a) through (e) until the entire track is completed. (Col. 3, lines 11-14)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Tagawa to include deleting the decrypted title key; deleting the media unique key; and repeating (a) through (e) until the entire track is completed. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Dolan (Col. 2, lines 27-28) in order not to compromise the decryption key.

Both references do not explicitly disclose a method of calculating a session key from the media unique key; and decrypting a doubly encrypted title key stored in the media with the session key to produce a singly encrypted title key.

Ansell in analogous art, however, discloses calculating a session key from the media unique key; (Col. 7, line 19) and decrypting a doubly encrypted title key stored in the media with the session key to produce a singly encrypted title key; (Col. 7, lines 19-22)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Tagawa and Dolan to include calculating a session key from the media unique key; and decrypting a doubly encrypted title key stored in the media with the session key to produce a singly encrypted title key. This modification would have been obvious because a person

Art Unit: 2133

having ordinary skill in the art would have been motivated to do so, as suggested by, Ansell (Col. 7, lines 20-22) in order not to have a secure communication between the media and the device.

As per claim 9:

Tagawa, Dolan and Ansell teach all the subject matter as discussed above. In addition, Tagawa further discloses a method wherein calculating the media key comprises:

dividing a media key block into chunks, (Col. 11, lines 59-64)
the chunks comprising bytes of encrypted data; (Col. 12, lines 17-61) and
encrypting a key within the media key block by setting the buffer to read at an offset within a specific chunk of the block. (Col. 9, line16-24)

As per claim 10:

Tagawa, Dolan and Ansell teach all the subject matter as discussed above. In addition, Tagawa further discloses a method wherein decrypting the key comprises:

(a) calculating a media key from first record; (Col. 9, lines 20-21) and
(b) updating the buffer offset; (Col. 12, lines 16-61; Col. 46, lines 14-16) and
(c) reading a second record at the updated buffer offset; (Col. 12, lines 16-61; Col. 25, lines 7-11; Col. 46, lines 14-16) and
(d) verifying the media key with a second record by comparing the calculated media key with a reference media key. (Col. 9, line 14-29)

As per claim 11:

Tagawa, Dolan and Ansell teach all the subject matter as discussed above. In addition, Tagawa further discloses a method wherein the buffer offset is determined by the type and length of the first record of the media key block. (Col. 12, lines 16-61; Col. 44, lines 15-21; Col. 46, lines 14-16)

As per claim 12:

Tagawa, Dolan and Ansell teach all the subject matter as discussed above. In addition, Tagawa further discloses a method wherein the group of frames comprises less than one second to about five seconds of decompressed and decoded audio content. (Col. 15, lines 59-65)

As per claim 38:

Tagawa and Dolan teach all the subject matter as discussed above. Both references do not explicitly disclose a system wherein the security engine further comprises a random number generator, the generator utilizing two or more system timers to create the random number.

Ansell in analogous art, however, discloses a system wherein the security engine further comprises a random number generator, the generator utilizing two or more system timers to create the random number. (Col. 9, lines 59-67)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Tagawa and Dolan to include a system wherein the security engine further comprises a random number generator, the generator utilizing two or more system timers to create the random number. This modification would have been obvious because a person having

Art Unit: 2133

ordinary skill in the art would have been motivated to do so, as suggested by, Ansell (Col. 2, lines 11-14) in order to have a system that restricts playback of the secure portable track and inhibit unauthorized copying.

As per claim 39:

Tagawa, Dolan and Ansell teach all the subject matter as discussed above. In addition, Tagawa further discloses a system wherein the generator increases the natural frequency update of the timer ticks used to create the random number. (Col. 9, lines 59-67 and Col. 10, lines 1-8)

9. Claims 33-34 and 36-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tagawa et al. (hereinafter Tagawa) United States Letter Patent Number 6,832,293 in view of Dolan et al. (hereinafter Dolan) United States Letter Patent Number 5,604,801 and further in view of Turgeon United States Publication Number 2003/0014371.

As per claim 33:

Tagawa and Dolan teach all the subject matter as discussed above. In addition, Tagawa further discloses a system comprising one or more engines for processing and transmitting audio, video or images, each engine comprising a secure application programming interface, the secure interface(s) for accessing the encrypted content and keys of the medium. (Col. 11, lines 65-67; Col. 12, lines 1-5)

Both references do not explicitly disclose a non-secure interface(s) for accessing the unencrypted content of the medium.

Art Unit: 2133

Turgeon in analogous art, however, discloses a non-secure interface(s) for accessing the unencrypted content of the medium. (Page 1, paragraph 12)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Tagawa and Dolan to include a non-secure interface(s) for accessing the unencrypted content of the medium. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so in order to make the system versatile by allowing access to demos and samples.

As per claim 34:

Tagawa, Dolan and Turgeon teach all the subject matter as discussed above. In addition, Tagawa further discloses a system comprising a security manager module. (Col. 8, lines 64-67; Col. 9, lines 14-24)

As per claim 36:

Tagawa, Dolan and Turgeon teach all the subject matter as discussed above. In addition, Tagawa further discloses a system comprising a device driver, the security engine accessing the content and keys through the device driver. (Col. 39, lines 42-50)

As per claim 37:

Tagawa, Dolan and Turgeon teach all the subject matter as discussed above. In addition, Turgeon further discloses a system wherein each of the one or more engines for processing and transmitting audio, video or images further comprising a non-secure application programming for accessing unencrypted content of the medium. (Page 1, paragraph 12)

Art Unit: 2133

10. Claim 35 is rejected under 35 U.S.C. 103(a) as being unpatentable over Tagawa et al. (hereinafter Tagawa) United States Letter Patent Number 6,832,293 in view of Dolan et al. (hereinafter Dolan) United States Letter Patent Number 5,604,801 in view of Turgeon United States Publication Number 2003/0014371 and further in view of Ansell et al. (hereinafter Ansell) United States Letter Patent Number 6,367,019.

As per claim 35:

Tagawa, Dolan and Turgeon teach all the subject matter as discussed above. Neither of the references explicitly disclose a system wherein the secure interface(s) communicate with the security manager module and module communicates with the security engine.

Ansell in analogous art, however, discloses a system wherein the secure interface(s) communicate with the security manager module and module communicates with the security engine. (Col. 12, lines 30-41; Col. 13, lines 1-26)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Tagawa, Dolan and Turgeon to include a system wherein the secure interface(s) communicate with the security manager module and module communicates with the security engine. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Ansell (Col. 2, lines 11-14) in order not to a system that restricts playback of the secure portable track and inhibit unauthorized copying.

Art Unit: 2133

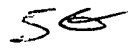
11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO Form 892.

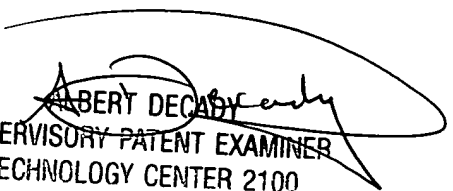
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shewaye Gelagay whose telephone number is 571-272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert Decady can be reached on 571-272-3819. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

04/15/05

Shewaye Gelagay 
Examiner
Art Unit 2133


ALBERT DECADY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100